common sense®

Global Policy
Comparative Report

Global Policy

Comparative Report

December 2021

Introduction

More than 40 years after their emergence, and through increasing dominance within our society, digital media technologies represent a double-edged sword. In the United States and many other countries, they have turbocharged economic growth, innovation, and civic participation, bringing disparate parts of the world closer together. At the same time, they have ushered in and accelerated new harms that degrade critical elements of our society's basic fabric. Individuals and families online today face a growing list of dangers, including the exposure to false, misleading, or damaging content, the unwanted capture and use of personal data for commercialization, and the addictive, destructive effects of social media on mental health.

At Common Sense, we have performed extensive research into how this increasingly digital world influences young people. In one sense, the results portray a bleak reality: Young users are **increasingly exposed to hate speech**, have **difficulties avoiding fake news items**, and are largely **unable to distinguish between advertising and other content**. Our studies also suggest, however, that online services provide social and academic benefits to young people and their parents. Even as it presents substantial, immediate risks to families, the double-edged sword of digital media can present them with powerful tools. Common Sense Media provides a **vast array of resources** to help young people, parents, and teachers navigate this dilemma. At the same time, we recognize that digital media has become so ubiquitous, complex, and embedded in our everyday lives that no individual user, parent, teacher, or nonprofit can tackle its significant harms alone. Rather, we **advocate** for swift and comprehensive government action, at federal and state levels, that will protect the digital rights of online users, especially young people.

We also recognize that online safety is not just an American issue. It is a global issue. Legislators around the world have started to take action in defense of digital consumers. Our allies abroad have not just talked about prioritizing the well-being of young users over the collection of online profits—they are passing laws to enforce such values. This report is an attempt to organize those efforts and compare them to legislation being discussed in the U.S. It is divided into three sections: **Platform Accountability**, **Privacy**, and **Healthy Design**. Each section describes the current situation for online users ("The Problem"), ideas proposed or enacted outside of the U.S. ("The Proposals, Abroad"), legislation inside the U.S. ("The Proposals, At Home"), and key commonalities or takeaways ("Recommendations"). Our overall aim is to give readers a clearer understanding of the global policy landscape regarding digital rights and to highlight some of the best practices that may shield users from digital violation, exploitation, and manipulation.

Platform Accountability

The Problem

Research shows that online content spreads fastest if it is extreme, violent, or misguided. Tweets with misinformation or disinformation items are 70% more likely to be shared than posts with accurate news (Science). Some social media platforms have taken advantage of this phenomenon: Recently disclosed internal reports at Facebook reveal how it deliberately designed algorithms to prioritize sensational posts (*WSJ*). **Such clickbait-oriented motivations have helped misinformation, disinformation, and hate speech move from the American fringe to the American home.** A 2017 Common Sense poll found that almost one third of children age 10–18 had shared fake news stories unknowingly, and only 44% could even identify fake news (CSM). Meanwhile, nearly two thirds of teens said they "sometimes" or "often" experienced sexist, homophobic, or religious-based hate content on social media in 2018 (CSM).

Members of minority or marginalized groups often experience these harms most intensely: Three in ten young women are "often" exposed to sexist comments, more than a third of young Black people are "often" exposed to racist comments, and more than four in ten LGBTQ+ youth "often" encounter homophobic posts online (CSM). Moreover, digital encounters with hate speech are on the rise: 23% of 14- to 17-year-olds said they "often" found racist comments on social media in 2020, nearly double the 2018 rate (CSM). **Fake news, conspiracy theories, and hate speech have infiltrated the increasingly digital lives of children and families. Social media business models that profit from toxicity, controversy, and attention are to blame.**

This is not just a concern for American families—the rise of misinformation, disinformation, and hate on the internet harms all Americans. Some 28% of respondents surveyed by the Anti-Defamation League in a 2020 national poll experienced "severe online harassment" (ADL). Between 2019 and 2020, three out of four women in North America reported witnessing online violence against other women (EIU). Digital offenses have real-life consequences: Higher rates of online hate speech have been shown to correlate with higher rates of offline hate crimes in American cities (NYU).

Fake news cultivated through social media also has hindered attempts to accurately inform the public about the COVID-19 pandemic, leading the WHO Director-General to warn of a concurrent "infodemic" (WHO). Indeed, a 2020 analysis in the U.K. found that over half of respondents who did not believe in the pandemic's existence cited Facebook as their primary news source (*Psychological Medicine*). Almost half of the 200 million tweets related to COVID-19 in the first few months of the pandemic were sent by bot accounts, many controlled by foreign entities hoping to sow confusion (NPR). Left unchecked, digital misinformation and disinformation are public health threats.

They also undermine the health of our democracy. In 2016, Russian groups exploited the unregulated digital landscape—one that saw Cambridge Analytica harvest data from 87 million Facebook accounts without consent—to spread false claims about American elections (*NYT*). Social media platforms have been so successful in amplifying false narratives that, as of April 2021, half of Republican voters still believe that the 2020 U.S. presidential election was "stolen" via voter fraud and that the deadly January 6 Capitol insurrection was nonviolent or organized by Antifa (Reuters). The lies and hatred that run rampant online have clear, damaging effects on our lives offline. **It is time to clean up the digital public square through comprehensive, fair regulation**

that prioritizes the well-being of our children, families, and democracy rather than the algorithmic optimization of attention and profit.

The Proposals, Abroad

Various regulations that target online misinformation, disinformation, and hate speech have been passed or proposed by our allies abroad.

Australia: Australia's legislature recently passed an **Online Safety Act** that directs its eSafety Commissioner to field claims of cyberbullying, cyber-abuse, and "abhorrent violent materials." The commissioner can impose civil penalties, criminal charges, ISP blocking requests, and transparency reporting to ensure compliance with proposed "Basic Online Safety Expectations," which seek to protect users from material that is violent or facilitates cyberbullying or cyber-abuse.

United Kingdom: U.K. lawmakers are discussing an **Online Safety Bill** that proposes a "duty of care" owed by large technology companies to their users. The bill grants the Office of Communications (Ofcom) the authority to enforce the removal of content that is "harmful," defined as carrying "material risk of the content having, or indirectly having, a significant adverse physical or psychological impact." The bill makes a clear distinction between content that is harmful for children and content that is harmful for adults, mandating that services "likely to be accessed by children" obey specific "duties to protect children's online safety" and "children's risk assessments" regarding potentially illegal or harmful content. Though the final details of the bill are under pre-legislative scrutiny, the drafted notion of "harmful" content is open to including misinformation and disinformation. Ofcom would be tasked with collecting and publishing transparency reports from service providers and managing a "super complaints" platform through which organizations can flag harm-inducing "systemic issues." Non-compliance fines would reach £18 million or 10% of global revenue.

European Union: The European Union's **Digital Services Act (DSA)** calls on member states to impose risk-assessment obligations on so-called "very large online platforms" (VLOPs) with at least 45 million monthly users in the E.U. These assessments, which would be sent to independent auditors, would force platforms to change products and architecture that create "systemic risks," including increased exposure to misinformation, hate speech, or other negative effects on the public health and on minors. The DSA would also harmonize content-removal contestation processes, propose a "trusted flagger" system, and introduce a set of risk mitigation measures that are content-agnostic. Non-compliance fees, imposed by the commission, can reach six percent of annual turnover. The DSA is set to work in tandem with the European Democracy Action Plan's updated "Code of Practice on Disinformation," which is currently being drafted and prioritizes increased data access for researchers.

Canada: Finally, officials in Canada plan to reintroduce **Bill C-36**, which would expand the Canadian Human Rights Act to protect against online hate speech. In its original form, the bill calls for a Digital Safety Commission to enforce the creation of internal procedural safeguards that provide service users with content moderation notices and flagging mechanisms. Content flagged as hate speech would need to be taken down within 24 hours if it meets the criteria of "detestation or vilification … that is stronger than dislike or disdain." The bill codifies a new digital protection order, called a "peace bond," the breach of which could carry up to a four-year prison sentence. The bill also allows regulators to levy CA$50,000 fines on individuals posting hate speech and grant CA$20,000 in reparations for hate speech victims.

The Proposals, At Home

Recognizing the serious threats of digitally circulated misinformation, disinformation, and hate speech, lawmakers in the United States have started to push for increased accountability from social media sites.

Sen. Edward Markey (D-Mass.) and Rep. Doris Matsui (D-Calif.A) introduced the **Algorithmic Justice and Online Platform Transparency Act** of 2021, aimed at forcing platforms to reveal how they harness user information and moderate content. The proposed bill calls for established algorithmic standards, algorithm-related record collection and sharing, and annual reports on content moderation practices. The bipartisan **Filter Bubble Transparency Act**, reintroduced by Sens. John Thune (R-S.D.), Richard Blumenthal (D-Conn.), Jerry Moran (R-Kan.), Marsha Blackburn (R-Tenn.), and Brian Schatz (D-Hawaii), would require large platforms to allow users to opt out of viewing information through a "filter bubble"—the array of obscure algorithms that amplify certain content depending on the user.

Reps. Jan Schakowsky (D-Ill.-) and Kathy Castor (D-Fla.) introduced the **Online Consumer Protection Act (OCPA)**, which would require online platforms to provide users with clear, transparent terms of service (TOS) agreements and to create consumer protection programs that set each platform's standards of conduct. The bill would give the FTC, state attorneys general, and individuals increased authority to take legal action and enforce civil penalties regarding potential violations. At the state level, **AB-587** in California would require social media sites to submit quarterly reports detailing TOS violations related to hate speech and misinformation, and to adopt policies to address such violating content. It would also provide a means for enforcing a company's posting and following of TOS agreements.

A few bills also seek to regulate through Section 230 reform. In their proposed **Platform Accountability and Consumer Transparency (PACT) Act**, Sens. Brian Schatz (D-Hawaii) and John Thune (R-S.D.) require accessible and clear acceptable-use policies, biannual content-moderation reports, and an open resource portfolio led by the National Institute of Standards and Technology. The bipartisan PACT Act would amend Section 230 of the Communications Decency Act to force large online platforms to remove illegal content within four days and to create defined complaint systems and due process protections for consumers. The **Justice Against Malicious Algorithms Act of 2021**, introduced by Rep. Frank Pallone Jr. (D-N.J.) and others, would remove Section 230 liability shields for large online platforms that knowingly or "recklessly" amplify content, through algorithms or other technologies, that "materially contributed to a physical or severe emotional injury to any person."

Sens. Mark Warner (D-Va.), Mazie Hirono (D-Hawaii), and Amy Klobuchar (D-Minn.) introduced the **Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms (SAFE TECH) Act**, which would remove Section 230 exemptions for online ads, paid content, and the enforcement of civil rights and cyber-abuse laws. Simply put, the SAFE TECH Act would mandate that if a platform profits from online material, they can be held liable for it. The SAFE TECH Act would also remove the liability shield for civil rights-infringing content, which is what Rep. Yvette Clarke's (D-N.Y.) proposed **Civil Rights Modernization Act of 2021** focuses on specifically. The **Protecting Americans from Dangerous Algorithms Act**, reintroduced by Reps. Tom Malinowski (D-N.J.) and Anna Eshoo (D-Calif.), seeks to remove liability immunity for large companies that use algorithms that amplify online civil rights abuses.

The amplification of hate speech on platforms that are directed at children could also be investigated and regulated by FTC and state attorney general audits under a reintroduced **Kids Internet Design and Safety (KIDS) Act**. This legislation, which would not change Section 230, calls for consumer reporting mechanisms and a publicly

accessible digital record of playable content. It would mandate the review of platform design effects on children and require platforms to provide clear guidance on kid-healthy content. Of particular concern is the ability of algorithms to push extreme content to young users.

Finally, Rep. Lori Trahan (D-Mass.) introduced the **Social Media Disclosure and Transparency of Advertisements (DATA) Act**, which would require large digital advertising platforms to create an ad library for academic researchers. Under this bill, platforms must report, among other things, each advertisement's targeting methods, audience descriptions, viewership numbers, and budgeting. The FTC would also be tasked with hosting a working group on researcher access and platform transparency. A bill introduced to the California State Assembly, **AB-1379**, would require similar libraries, calling for each large platform to create an ongoing record of audience descriptions and online advertisements and to design an application accessible to third parties so they can analyze potential discrimination and bias in targeted political ads.

Recommendations

To compare platform accountability policies across borders, it is important to contextualize national and regional differences. Countries outside of the U.S. do not have to consider Section 230, for example, and freedom of speech is not as absolute in its protection abroad as it is under the First Amendment. Still, the laws and proposals listed above share many notable principles as they address online misinformation, disinformation, and hate speech.

First, it is clear that governments around the world are interested in strengthening protections for young users. The Online Safety Bill's explicit distinction between children and adults gives Ofcom a more nuanced ability to confront content that may pose particular harms to young people in the U.K. In the U.S., the reintroduced KIDS Act, with its calls for algorithm audits and family resources, stands as a comprehensive, kid-specific framework that could limit young users' exposure to hate speech and fake news. Lawmakers in the European Parliament are also introducing specific protections for kids in their DSA proposals. **Policymakers should learn from these proposed measures to reduce or end the amplification and targeting practices that threaten the healthy development of young people in the name of profit**.

Second, regulators across the board demand increased platform transparency. From the Online Safety Act's service provider reports, to the DSA's risk assessments, to the FTC support proposed in Congress, the push for external audits may force platforms to open the black box that has helped produce divisive, damaging, and misleading online spaces. Different roads could lead to this goal, including mandatory ad libraries, trade secret protection waivers, enhanced enforcement mandates of existing agencies, and the creation of new intermediaries to vet researchers. These roads give researchers, regulators, and individuals the opportunity to evaluate and improve the internet's complex, powerful processes.

Another crucial component of platform transparency and moderation policy is the provision of clear and accessible complaint mechanisms, flagging systems, and TOS agreements. Some legislation, like the U.K.'s Online Safety Bill, details the need for (and support of) human moderators working alongside artificial intelligence systems. **Each platform must make it clear how and why users receive content, must enable qualified researchers to test and study the platform's internal workings, and must facilitate a straightforward process through which content may be flagged and removed, albeit with equally straightforward appeals mechanisms**.

Third, recent legislation mandates accountability alongside transparency. Tech companies are required to follow regulator-developed, sector-specific codes of practice under existing or forthcoming online safety legislation in Australia and the U.K. These codes favor human well-being—some sort of "duty of care" toward consumers. In the U.S., legislation like the SAFE TECH Act and the Civil Rights Modernization Act has been proposed to deny Section 230 liability shields for platforms that evade such a duty by hosting or amplifying content that either profits from users or opposes their best interests. Bills like the PACT Act, the Online Consumer Protection Act, and AB-587 focus on the accessibility and enforcement of TOS agreements. These proposals echo sections of the DSA and the Online Safety Bill, which would require platforms to implement terms and conditions consistently, in a "diligent, objective, and proportionate manner." **Given their sweeping influence and varying content, large tech companies need to be held accountable in their efforts to enforce on-site rules and protections that keep users safe.**

Throughout these ideas runs a global recognition that **regulation will be most effective if it addresses issues of misinformation, disinformation, and hate speech at a systemic level**. Rather than punish cases in a whack-a-mole, after-the-fact manner, lawmakers seek to design preventative measures to tackle the structural roots that permit, condone, and amplify harmful content. In Europe, the DSA embodies this approach with its systemic risk assessment mandates. The American bills that promote the creation of defined complaint systems, algorithmic standards, and TOS violation strategies also push platforms to diagnose and treat cancer-like online material before it spreads throughout society.

Privacy

The Problem

As our professional and social lives have become increasingly digital, our personal information has become increasingly controlled by large online platforms. With few state laws and no comprehensive federal laws protecting fundamental internet privacy principles, corporations like Facebook and Google have collected and sold the data of American citizens without explanation or consent for years. In doing so, companies have shown a blatant disregard for user privacy. Even when iPhone users ask apps not to track their activity, for example, those apps use so-called "fingerprinting" techniques to collect as much personal information as possible (*WaPo*). **The lack of legislated privacy protections in the United States has been devastating, as unregulated data trafficking facilitates foreign interference in elections, a culture of surveillance and the manipulation of individuals, and a rising number of cyberattacks**.

Digital privacy risks are particularly concerning for children and teens. Given their extensive screen and internet consumption, young people are the most surveilled and tracked generation ever. They use the internet to access sensitive health information, have intimate conversations, and stay informed (CSM). At the same time, online services used by teens and children are often the most intrusive, incessantly harvesting their personal material. When compared to the average app, apps aimed at teens contain "more third-party trackers and request more permissions to data, including those defined as 'dangerous' permissions" (BBB). These apps are also more likely to rely on advertising to earn revenue (83% of teen apps, compared to 51% of all apps; BBB), feeding into a $1.7 billion digital advertising market for kids (SuperAwesome/PWC). These ads are often manipulative or inappropriate for young users, many of whom cannot distinguish between advertising and other content (over 75% of kids age 8–11 cannot; CSM). **In the face of widespread, youth-oriented data exploitation, America's existing privacy laws are outdated, ill-equipped, and underenforced**: Half of free apps serving kids were found to serve COPPA-violating ads in a 2018 study (Reyes, et al.).

Privacy breaches are not background noise—digital users of all ages understand the risks and want more protections. A recent survey of 1,000 U.S. parents found that 98% are concerned about their kids' digital privacy (Startpage). Sixty-one percent of teens have at least heard of the Facebook-Cambridge Analytica controversy, and around eight in ten have strengthened their privacy settings on a social networking site (CSM). Ninety-four percent of teens and 97% of parents say it is "important" for sites to ask permission before selling or sharing their personal information (CSM). And the widespread corporate failure to disclose data collection methods is not lost on users, which is why over 90% of parents and teens want websites to label how personal information is collected and handled (CSM). **On the whole, the numbers make clear that families across the country seek increased, comprehensive online privacy rights, including special protections for vulnerable young users.**

The Proposals, Abroad

Other countries have a range of digital privacy regulations in place.

European Union: Since 2018, the General Data Protection Regulation (GDPR) has mandated a minimum level of protection for internet users in the E.U. Key GDPR principles include mandatory informed consent to data processing, the right of access to data processing tactics, data minimization and purpose limitation, the right to be

forgotten, the right to deletion and correction, and special provisions for young people such as parental consent for processing data of children. Penalties can reach €20 million or four percent of global revenue.

The upcoming **Digital Services Act** (DSA) and **Digital Markets Act** (DMA) will not directly address individual privacy rights, but could introduce a ban on manipulative design techniques that trick people into consenting to terms of service agreements. The DMA will likely require user consent (via the GDPR) for sharing personal information across services—between Facebook, Instagram, and WhatsApp, for example.

Nations have added additional measures in their adoption of the GDPR, especially regarding young internet users.

United Kingdom: In the face of Brexit, the U.K.'s **Data Protection Act 2018** implemented GDPR privacy components. This act also tasked the Information Commissioner's Office (ICO) with creating a set of standards for young internet users. The resulting **Age Appropriate Design Code**, also known as the Children's Code, sets out 15 principles, including prioritizing best interests of the child, data minimization, and "privacy by default" settings, which together present a risk-based approach to data protection for any services "likely to be accessed by children" in the U.K.

The Children's Code is a useful benchmark, and its influence has been immediate and global: To prepare for its September 2021 enforcement date, Instagram began asking users their age, Google offered teens the right to be forgotten, and TikTok enhanced its direct-message privacy settings (***Wired***).

Many are following the U.K.'s lead. France, for example, requires that terms and conditions must be easily accessible to children, that online service providers offer enhanced privacy settings by default, and that age verification (AV) and parental control systems are proportional, standardized, robust, and privacy-preserving. The Netherlands mandates children-focused privacy designs, child rights privacy impact assessments, and the avoidance of exploitation of children at all times.

Irish lawmakers, meanwhile, have proposed a "floor of protection," upon which service providers can offer additional tools like AV. They advocate for child-oriented transparency, a prohibition on child profiling, and a stance that young users cannot consent as if they were adults.

Some countries, like Sweden, directly incorporate ideas from **UN General Comment 25**, namely nondiscrimination, the child's best interest, the child's right to survival and development, and a respect for the views of the child.

The Proposals, At Home

Given the public need and popular demand for revamped digital privacy regulations in the U.S., a number of measures have been passed or proposed at state and federal levels.

In 2018, the California legislature passed the **California Consumer Privacy Act (CCPA)**, which went into effect January 1, 2020. The CCPA gave 40 million consumers unprecedented privacy protections, including the right to know what personal information is collected by service providers and what they do with it, the right of access, transfer, and deletion, and the right to opt out of the sale of their data. The CCPA authorizes a private right of

action, allowing users to sue companies regarding data breaches. Through CCPA, children under 16 in California must opt in to authorize the sale of their information, and children under 13 need parental consent. Proposition 24, or the California Privacy Rights Act of 2020 (CPRA), expands CCPA's reach on personal data protection—for example, offering opt-out rights with respect to the use of sensitive data. In the wake of CCPA, dozens of states have proposed data privacy legislation, but only two have passed: the Virginia Consumer Data Protection Act and the Colorado Privacy Act.

In 2019, Sen. Maria Cantwell (D-Wash.) spearheaded the Consumer Online Privacy Rights Act (COPRA), which set out to give digital users fundamental protections, including the right to be free from deceptive and harmful data practices and the right to access, control, delete, correct, and transfer their data. The bill provided a privacy floor upon which states could enhance privacy rights and created special standards for the collection of sensitive biometric and geolocation data while bolstering the FTC's enforcement authorities.

A year later, Sen. Sherrod Brown (D-Ohio) introduced the Data Accountability and Transparency Act of 2020 (DATA 2020). DATA 2020 attempted to transfer the burden of privacy protection from consumers to corporations by limiting the collection of data to specific legal purposes that companies must prove. It also set out civil rights protections for personal data use, permitted attorneys general to enforce more protective state laws, and proposed an independent federal agency that could issue penalties for noncompliance.

This year, Sen. Brian Schatz (D-Hawaii) and 17 other senators reintroduced the Data Care Act of 2021, which would impose a "duty of care" on providers handling identifying information. This quasi-fiduciary duty would require companies to secure personal data, inform users of data breaches, refrain from using data to harm users, and ensure that such care extends to third parties that handle the data. Sen. Ron Wyden's (D-Ore.) Mind Your Own Business Act of 2021, which would mandate periodic reporting and opt-out processes for "high-risk" information or automated decision-making systems, would also codify executive responsibility by leveraging criminal penalties for false certification by corporate officers. The bill would extend enforcement capabilities to advocacy organizations, enabling more fulsome enforcement.

Strengthening digital privacy rights is not just a Democratic issue—it has support from both sides of the aisle. The Social Media Privacy Protection and Consumer Rights Act of 2021, introduced by Sens. Amy Klobuchar (D-Minn.), John Kennedy (R-La.), Joe Manchin (D-W.Va.), and Richard Burr (R-N.C.), would give individuals the right to opt out of data tracking and collection. Meanwhile, Sens. Roger Wicker (R-Miss.) and Marsha Blackburn (R-Tenn.) introduced the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act, which calls for consent to process personal data for users up to 16 years old, the right to access, delete, correct, and transfer data, and the minimization of data collection.

In May 2021, Sens. Ed Markey (D-Mass.) and Bill Cassidy (R-La.) introduced the Children and Teens' Online Privacy Protection Act (CTOPPA). This bipartisan bill is also referred to as "COPPA 2.0" because it proposes critical updates to the Children's Online Privacy Protection Act of 1998 (COPPA). Among other things, CTOPPA would require providers to obtain consent for data collection of users up to age 16 and would revise COPPA's "actual knowledge" threshold to a "constructive knowledge" standard that would prevent sites from pretending they do not have young users and protects kids and teens where they are. The act would also place a ban on targeted ads directed at kids, enact a right to erase children's personal information, establish a Youth Marketing and Privacy Division at the FTC, and bolster the security and transparency standards for children's connected devices.

Another proposed COPPA revamp comes in the form of the **Protecting the Information of Our Vulnerable Children and Youth Act (Kids PRIVCY Act)**, introduced by Rep. Kathy Castor (D-Fla.). This bill would protect all minors under 18 and combine elements of COPPA (requiring parental consent on certain sites for kids under 13) with the U.K.'s Age Appropriate Design Code (requiring that sites "likely to be accessed" by teens or children prioritize the best interests of those users and incorporate risk-based protections). The Kids PRIVCY Act would also require concise and user-friendly privacy policies, allow the FTC and parents to seek civil damages, ban forced arbitration, and ban targeted ads for children and teens.

Facilitating the enforcement of privacy laws is another area of congressional focus. Many bills seek to bolster the FTC in this vein. Rep. Kathy Castor's (D-Fla.) **21st Century FTC Act** would grant the agency notice and rulemaking authority with respect to unfair or deceptive acts or practices under the Administrative Procedure Act (APA). Meanwhile, the **Consumer Protection and Recovery Act**, introduced by Tony Cárdenas (D-Calif.), would give the FTC clear leverage to hold wrongdoers accountable for manipulative and fraudulent practices in marketplaces.

Some legislation proposes the creation of a new federal privacy agency altogether to manage and enforce bolstered privacy rights. In the **Data Protection Act of 2021**, Sen. Kirsten Gillibrand (D-N.Y.) calls for a Data Protection Agency in the executive branch to regulate the collection of personal information online. In 2020, the CPRA successfully established a California Privacy Protection Agency, which now has a five-member board, holds informational hearings, seeks public consultations, and enforces state privacy laws.

For all their titles and acronyms, these bills make one thing clear: **There is state-level precedent and bipartisan momentum to heed the call of American families by enacting legislation that will safeguard all individuals' basic rights to digital privacy and grant additional protections for young people**.

The Recommendations

Compared to the U.S., many countries have stronger foundations of privacy rights that underpin digital laws. Privacy is constitutionally protected by the European Convention on Human Rights (**Article 8**) and the E.U. Charter of Fundamental Rights (**Article 7**). Indeed, Article 8 of the Charter specifically addresses the right to the protection of personal data. The Constitution of the United States, meanwhile, makes no mention of privacy or personal data. To keep up with the increasingly sophisticated and invasive nature of online services, the digital privacy rights of Americans need to be expanded. Data privacy protections must be made explicit and federal.

First, new measures must be age appropriate, placing particularly strong protections around young users, including teenagers. As the GDPR and CPRA mandate, and as the Kids PRIVCY Act and CTOPPA propose, privacy must be the default setting for all children and teens up to 18 years old. Certain features, like geolocation tracking and behavioral advertising, should be turned off for minors. These bans on youth exploitation are already in force abroad (in the U.K., for instance) and have been advocated for at home (with California already offering special protections to teens). On the whole, privacy laws should push large online service providers to follow UN General Comment 25 and prioritize the child's best interest in online design. The privacy of young users must no longer be a source of deceitful and profitable ignorance for online platforms. This privacy must be a default and a design feature, something built from the ground up through every stage of product development.

Teenage users must be given autonomy to make data decisions for themselves, meaning that companies need to provide graduating, age-specific control levels and language styles, as suggested by the Kids PRIVCY Act's "Young

Consumer" designation. **Platforms also must be held accountable for understanding their users' ages**. This requirement comes through in the U.K.'s Age Appropriate Design Code and the Kids PRIVCY Act, which cover any services "likely to be accessed" by children. CTOPPA would also prevent sites and apps from turning a blind eye to young users by mandating a "constructive knowledge" threshold in which platforms are assumed to know audience ages. As recommended in France, comprehensive age assurance and verification systems should be required and designed in ways that do not subvert privacy or anonymity.

These youth provisions should be part of a federally enforced privacy floor so that everyone is protected. A national privacy law should, like the GDPR, prioritize data minimization and user rights. Users should have the ability to freely access, correct, delete, and transfer such data. These measures would mirror and go beyond those enforced in California under CCPA and CPRA. In line with the GDPR, Children's Code, COPRA, DATA 2020, and other enacted or proposed laws, data minimization to what is reasonably necessary for a service should be incentivized and enforced. A legal purpose should be mandatory for each sale, transfer, or other use of data. As technology keeps moving, however, states need to be able to iterate—we therefore need a floor, not a ceiling, on which states can provide additional safeguards.

A national privacy law should require TOS agreements to be accessible in languages appropriate to their audience. They also must be easily enforceable, consistently reported, and regularly updated. Finally, effective legislation must designate strong enforcement mechanisms through increased regulator support and avenues for a private right of action. **An independent privacy enforcer, either within or outside of the FTC, is needed to maximize the individual and societal benefits of comprehensive digital privacy frameworks**. The entity must be well funded to hire skilled technologists and sufficiently authorized to create and update regulations in a rapidly changing field. It must be empowered to fine companies meaningful amounts and to seek fair redress for individuals.

This support will give regulators and citizens effective means for holding providers accountable so that the personal data of all Americans—especially children and teens—is respected and protected rather than trafficked and abused.

Healthy Design

The Problem

The individual damage and societal risk from powerful platforms do not result from groups of businesses making innocent, surface-level decisions to take advantage of regulation vacuums. Every day, global tech companies actively organize thousands of psychologists and engineers to direct and manipulate individuals—to not only track and understand our behavior, but also to influence and determine it. They pull off this manipulation using a sophisticated arsenal of design techniques. **As they reduce our "right to the future tense" (Zuboff), unhealthy design features facilitate, reinforce, and aggravate privacy and platform accountability harms (as described in the previous sections)**.

Large service providers have built platforms in such a way that they actively spread hate speech, misinformation, and disinformation. In order to optimize clicks and attention, these companies employ algorithms that amplify particularly controversial content. Facebook, for example, has systematically tinkered with its news feed to boost posts with more reshares and comments, in effect promoting divisive, often misleading content (*WSJ*). These profit-driven decisions compromise American democracy. In the lead-up to the 2020 presidential election, 22 of the top 50 most popular Facebook posts presented false or misleading assertions about voting (ProPublica). The spread of harmful content is not beyond the control of platform designers: Researchers have shown how changing targeted advertising tactics can reduce a platform's volume of fake news (MIT). Indeed, these **companies have the power—the obligation—to improve platform designs so that they no longer exploit biases and extend toxicity**.

Manipulative design also undermines consumer privacy. Social plug-ins, such as Facebook's "like" button, push internet users to share large amounts of data unknowingly. Researchers have uncovered how large service providers guide users to disclose personal information through privacy-light default settings, confusing or frustrating interfaces, coercive wording, and the illusion of choice (Norwegian Consumer Council). **Deceptive design features nudge users toward privacy-invasive options, essentially allowing companies to steal their data.** The responsibility for curtailing unhealthy design cannot be on individuals, for these nudges work even when users are aware they are being nudged (University of Hamburg).

If nothing changes, **the sinister architecture underlying popular platforms will continue to wreak particular havoc on some of the internet's most vulnerable users: young people**. Algorithmic amplification can push harmful and illegal content, from sex and drugs to violence and hate speech, onto the screens of kids and teens (*WSJ*). Certain digital features coerce children into spending money: "Advergames" slip commercial content and brands into the emotional experience of playing games; "host selling" uses friendly characters to push products on young users that have become attached to the characters; and hidden elements advertise behind an influencer or are not clearly labeled. These tactics exploit the data, attention, and integrity of young users, many of whom cannot distinguish between advertising and other content.

As platforms design services to maximize the user's time spent online through autoplay, infinite scroll, "streaks," push alerts, and badge rewards, they manipulate the developing minds of kids and teens. Many become addicted to their screens. The age at which this addiction can begin is strikingly low. On average, kids under 8 consume almost two and a half hours of digital media per day, and over two thirds of 5- to 8-year-olds have their own tablet or smartphone (CSM). Recent reports emphasize how addictive design features, like the quantification of

popularity through follower counts, can exacerbate social media's negative mental health effects on our youth. Facebook is aware of these harms. It has secretly researched and quantified them: An internal study found that around thirteen percent of British teens and six percent of American teens reporting suicidal thoughts traced them to Instagram (*WSJ*).

Social media's existing infrastructure has been made in obscure, unhealthy, and manipulative ways. This shady foundation may serve corporate interests, but it goes against the best interests of American consumers and American society. **Like the buildings we inhabit offline, the sites we inhabit online must fall under a proper code of regulation, one that favors human welfare rather than shareholder gain**.

The Proposals, Abroad

In their efforts to regulate harmful content and privacy abuse online, many of our allies have mandated healthy design practices. In addition to stipulating that a data subject's consent be freely given, specific, informed, and unambiguous, the GDPR promotes the importance of data protection "by design and by default." Companies have tried to subvert these principles by nudging users toward giving consent or accepting lower privacy settings (Utz, et al.), leading nations like Ireland, France, and the U.K. to add explicit restrictions on consent nudging to their GDPR implementation.

United Kingdom: As suggested in its name, the U.K.'s Age Appropriate Design Code sets out design standards that prioritize the child's best interests. In addition to bans on consent nudges, these include high privacy default settings, deactivated geolocation default settings, and clear indications when geolocation or parental controls are turned on.

European Union: According to the Netherlands' new Code for Children's Rights, children should be involved directly in the entire design process of digital products. The code requires companies to embrace "child-friendly privacy design," which includes allowing users to remain anonymous and requiring profiling, microphone, and camera setting defaults to be turned off. Economic exploitation of children must be avoided, meaning that in-app purchases should require parental consent and all games with in-app purchases must not be labeled as "free." Harmful and addictive design must be avoided, meaning that services should not, for instance, automate the display of violent or hateful content, they should not constantly notify kids, and they should let players take breaks without having to restart games. The Dutch code also calls for the development of industry guidelines to protect the rights and interests of young internet users.

Australia: This call has been made elsewhere as well with respect to digital users of all ages. Australia's Online Safety Act mandates that the eSafety Commissioner oversee the creation of codes and standards for each section of the digital industry. The Commissioner is also charged with continuing the Safety by Design (SbD) initiative, which has already resulted in an SbD Framework, SbD Principles, SbD self-assessment tools, and an SbD Investment Checklist for companies. Some SbD best practices include high-level privacy settings and verification systems, comprehensive warning and flagging mechanisms, and the use of human moderators alongside algorithms.

The U.K.'s Online Safety Bill includes a provision that the government create its own guidance frameworks to support product designers, managers, and developers as they incorporate safety-by-design approaches. Such

knowledge collection and sharing could help companies design systems to maximize privacy and reduce the amount of illegal content on their platforms.

At the E.U. level, the Digital Services Act would approach healthy design from a risk mitigation angle. The reasonable measures that VLOPs would need to implement to avoid "systemic risks" include the adaptation of interface design and service functions. On the other hand, VLOPs would face regulation following evidence that particular algorithm designs or decision-making processes contribute to the infringement of privacy rights or the dissemination of information with negative effects (on public health, security, or elections). The final details regarding the DSA, including stipulations on platform design, are still being negotiated by the European Council and Parliament.

The Proposals, At Home

Existing bills proposed in the U.S. have incorporated many of the healthy design regulations put in place abroad.

The Children and Media Research Advancement Act (CAMRA), introduced by Sen. Ed Markey (D-Mass.), would authorize the National Institutes of Health to fund research about the impact of media, including social media, on the cognitive, physical, and social-emotional development of young users. The bill, which has bipartisan support, would allow experts to better understand links between platform design and child well-being.

The Kids PRIVCY Act adopts elements of the U.K.'s Age Appropriate Design Code and would require platform architects to make the best interests of children and teenagers a "primary design consideration" as they develop user-friendly privacy systems. The KIDS Act of 2021 would directly ban manipulative design features that take advantage of users under 16, including autoplay, push alerts, badge rewards, "like" buttons, and follower counts. It would prohibit the amplification of harmful content on websites for kids and teens and would require websites to create tools for reporting when such content is recommended to young users. It would also stop websites from promoting certain marketing components—unboxing videos, tobacco and alcohol ads, and embedded interactive elements—to kids and teens. Furthermore, the KIDS Act would require regular examination of how platform design, algorithmic amplification, and advertising can affect children's digital well-being. The KIDS Act would expand to a federal level prohibitions on ads targeted to minors for products that cannot be legally sold to them. Such bans have been enforced on a state level for years through California's "Eraser Button" law and the Delaware Online Privacy and Protection Act.

Another piece of federal legislation pushing for healthy digital design is the Deceptive Experiences to Online Users Reduction (DETOUR) Act, introduced by Sens. Mark Warner (D-Va.) and Deb Fischer (R-Neb.). This bipartisan act seeks to prevent large online platforms from using manipulative design tactics to deliberately hinder user autonomy. More specifically, it would authorize the creation of an FTC-registered professional standards group that could investigate and promote best practices regarding user design, prohibit design that leads to compulsive usage in children under 13, prohibit companies from running behavioral experiments on users without informed consent, and direct the FTC to develop industry rules regarding informed consent, independent review boards, and professional standards bodies. The Algorithmic Justice and Online Platform Transparency Act also calls for the establishment of industry-wide algorithmic standards.

Finally, two bipartisan bills promote specific design safeguards. The Children and Teens' Online Privacy Protection Act (CTOPPA) would mandate that connected devices indicate whether they have parental controls

on privacy dashboards, and the **Filter Bubble Transparency Act**, with its "filter bubble" opt-out button, aims to harness digital design to prevent harmful amplification processes.

Finally, recent amendments to the **California Consumer Privacy Act** include a ban on the use of manipulative design to obtain data processing consent. The amendments explicitly prohibit opt-out forms from containing confusing language, more steps than opt-in forms, encouragements not to opt out, or lengthy text that requires scrolling. The California Privacy Rights Act also bans manipulative design features that subvert informed consent. Lawmakers in other states, like Washington, have tried but failed to pass legislation regulating manipulative design.

Recommendations

Internet users need legislation that defends them from the cunning and misleading design tactics that companies use to thwart privacy and spread harm for commercial gain.

First, any future federal privacy law requiring informed consent for the sale of personal data online must include specific prohibitions on manipulative design practices that nudge individuals to give consent or offer up more information than desired. The ban would prevent children in particular from being tricked into giving up more information than suits their best interests and from giving away what little privacy protection they have. In doing so, American lawmakers would follow the lead of many European counterparts who have adapted to the increasingly complex nature of platform architecture.

But policy must go beyond a focus on consent nudging to remedy other design components that hinder the healthy development of young people. As laid out in the children codes of the U.K. and the Netherlands, and as proposed in the KIDS Act of 2021, features like autoplay, push and badge alerts, and infinite scroll should be seriously limited, if not banned, on services used by kids and teens. **Legislation must put an end to the addictive design that encourages compulsive use among young people**. Lawmakers should also consider prohibiting design elements, including follower counts and "like" buttons, that quantify popularity and exacerbate social comparisons among young users.

Design regulation abroad clearly promotes the idea that children should not be economically exploited in any form while using the internet. Similar principles must be adopted in the U.S. to protect the dignity and well-being of vulnerable young users. **Platforms should be barred from encouraging or coercing children to spend more money online** through embedded interactive marketing tactics, confusing mixtures of real and virtual currency, hosts that shame users into buying, and advergames that conflate play with product. By taking action now, we can ensure that the digital lives of children are free from commercial abuse.

Whereas protections in European nations like France call for robust, nuanced parental control systems, these features are largely missing from legislation in the U.S. As a result, millions of American children and teens currently have frictionless access to hundreds of thousands of apps, many of which contain inappropriate or violent content. Mandating parental control settings, ones that clearly indicate to young users when they are turned on, would prevent them from being exposed to harmful material while respecting their autonomy and dignity.

Overall, **legislation should mandate that large online platforms consider the best interests of children and teens throughout the full development process of their products and services**. The Kids PRIVCY Act, DETOUR Act, and Algorithmic Justice and Online Platform Transparency Act make this stipulation explicit, as do various European codes. A promising method for ensuring that the perspective of children is made primary would be to create industry standards for algorithm design and transparency. Authorized support for scientific research about the influence of online platforms on child development, as laid out in CAMRA, will be crucial to setting these healthy standards. Australia's Safety by Design initiative is also a strong model that American regulators and businesses can follow to work together and develop frameworks of best practices for specific sections of the digital industry. The creation and updating of these guidelines will provide meaningful opportunities for domestic and international collaboration and competition through which the internet can become a safer and more productive place.

Conclusion

Perhaps the most important takeaway across the issues addressed above—Platform Accountability, Privacy, and Healthy Design—is that they are fundamentally intertwined. They connect in terms of the respective harms posed by inadequate regulation (user data collected without consent, for instance, feeds the amplification algorithms designed to promote online toxicity) and the prospective solutions (preventing the capture of data without consent may reduce such toxicity). Indeed, the final section on Healthy Design offers structural remedies that would ameliorate many of the problems presented in the first two sections, and passing privacy protections would likewise go a long way toward curbing platform abuses and problematic design. Legislation should ensure that the reduction of misinformation, disinformation, and hate speech, and the enhancement of consumer privacy and safety, are baked into platform design and offered as default settings. More generally, lawmakers should take into account all three elements when drafting or considering any digital rights bill.

In addition, it is important to recognize the significant overlap between the motivations of policymakers at home and those abroad. While there are different constraints in the U.S. (e.g., the First Amendment; privacy not being recognized as a fundamental right), there is considerable agreement about the immense amount of work needed to protect users from exploitative online platforms and the potential measures that can be implemented to that end. Above all, there is a shared understanding that bold, widespread action is needed immediately. After years of falling behind while allies enacted reasonable standards to protect their citizens, the U.S. now has an opportunity to set a global example by protecting the digital safety and integrity of all Americans, young and old.